

2766 #3
Priority
Pym
4-1
3.3.02
500.38035X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): H. KURUMATANI
Serial No.: 09/468,948
Filed: December 22, 1999
Title: METHOD AND APPARATUS FOR ELLIPTIC CURVE
CRYPTOGRAPHY AND RECORDING MEDIUM THEREFOR
Group:

RECEIVED
FEB 16 2000
TO 2100 (MAIL ROOM)

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

February 11, 2000

Sir:


Under the provisions of 35 USC 119 and 37 CFR 1.55, the
applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 10-364277
Filed: December 22, 1998

A certified copy of said Japanese Patent Application is
attached.

Respectfully submitted,

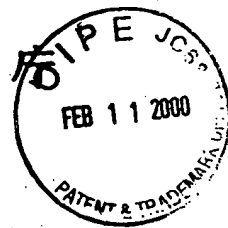
ANTONELLI, TERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No. 29,621

CIB/ssr
Attachment

日本国特許
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

1998年12月22日

願番号
Application Number:

平成10年特許願第364277号

願人
Applicant(s):

株式会社日立製作所

RECEIVED
FEB 16 2000
TC 2100 MAIL ROOM

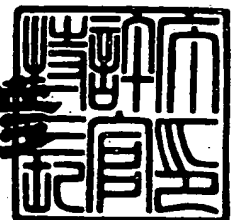
CERTIFIED COPY OF
PRIORITY DOCUMENT

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年12月10日

特許庁長官
Commissioner,
Patent Office

近藤隆彦



出証番号 出証特平11-3086373

【書類名】 特許願

【整理番号】 K98013811

【提出日】 平成10年12月22日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明の名称】 楕円曲線暗号実行方法及び装置並びに記録媒体

【請求項の数】 7

【発明者】

 【住所又は居所】 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所 ソフトウェア事業部内

 【氏名】 車谷 博之

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100068504

 【弁理士】

 【氏名又は名称】 小川 勝男

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 楕円曲線暗号実行方法及び装置並びに記録媒体

【特許請求の範囲】

【請求項 1】

楕円曲線が $y^2 + xy = x^3 + ax^2 + b$ である、2 の拡大体上の楕円曲線暗号の実行方法であって、各座標成分が前記楕円曲線上の点である点 $P_1(x_1, y_1)$ 、 $P_2(x_2, y_2)$ の加算を $P_3(x_3, y_3)$ とし、点 $P_1(x_1, y_1)$ 、 $P_2(x_2, y_2)$ の減算を $P_4(x_4, y_4)$ とした場合、前記 x_1 を入力するステップと、前記入力された x_1 を射影空間の X 座標、 Z 座標 $[X_1, Z_1]$ に変換するステップと、前記射影空間の座標 $[X_1, Z_1]$ を記憶するステップと、前記 x_2 を $[X_2, Z_2]$ に変換するステップと、前記 $[X_2, Z_2]$ を記憶するステップと、前記 x_4 を $[X_4, Z_4]$ に変換するステップと、前記 $[X_4, Z_4]$ を記憶するステップと、前記記憶された $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ から $[X_3, Z_3]$ を求めるステップと、前記 $[X_3, Z_3]$ から x_3 に変換するステップと、前記 x_3 を出力するステップとからなり、点 $P_1(x_1, y_1)$ のスカラー倍を計算することを特徴とする楕円曲線暗号実行方法。

【請求項 2】

請求項 1 記載の楕円曲線暗号実行方法であって、乱数 k を生成するステップと、前記生成された乱数 k を記憶するステップと、 x 座標を射影座標に変換した後、射影空間の各座標成分と前記記憶された乱数 k と演算させて、射影座標 $[k^2 x, k]$ に変換するステップとを有することを特徴とする請求項 1 記載の楕円曲線暗号実行方法。

【請求項 3】

請求項 1 記載の楕円曲線暗号実行方法であって、乱数 k を生成するステップと、前記生成された乱数 k を記憶するステップと、 x 座標を射影座標に変換した後、射影空間の各座標成分と前記記憶された乱数 k と演算させて、射影座標 $[kx, k]$ に変換するステップとを有することを特徴とする請求項 1 記載の楕円曲線暗号実行方法。

【請求項4】

請求項1記載の楕円曲線暗号実行方法であって、記憶された $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ から x^3 に変換できる $[X_3, Z_3]$ を求めるステップには、 $B = X_1 Z_2^2 + X_2 Z_1^2$ を計算するステップと、前記計算された B を記憶するステップと、前記記憶された B を $B = 0$ であるか否かを判別するステップと、 $B = 0$ の場合は無限遠点を出力し、 $B \neq 0$ の場合は $Z_3 = Z_4 B$ を計算するステップと、前記計算された Z_3 を記憶するステップと、前記記憶された Z_3 から $X_3 = X_4 Z_3^2 + X_1 X_2 Z_1^2 Z_2^2 Z_4^2$ を計算するステップとを有することを特徴とする請求項1記載の楕円曲線暗号実行方法。

【請求項5】

請求項1記載の楕円曲線暗号実行方法であって、記憶された $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ から x^3 に変換できる $[X_3, Z_3]$ を求めるステップには、 $B = X_1 Z_2 + X_2 Z_1$ を計算するステップと、前記計算された B を記憶するステップと、前記記憶された B を $B = 0$ であるか否かを判別するステップと、 $B = 0$ の場合は無限遠点を出力し、 $B \neq 0$ の場合は $Z_3 = Z_4^2 B^2$ 及び $X_3 = X_4 B^2 + X_1 X_2 Z_1 Z_2 Z_4^2$ を計算するステップとを有することを特徴とする請求項1記載の楕円曲線暗号実行方法。

【請求項6】

楕円曲線が $y^2 + xy = x^3 + ax^2 + b$ である、2の拡大体上の楕円曲線暗号の演算装置であって、乱数 k を生成する乱数生成部と、2の拡大体上の座標 x_0 と前記乱数 k とを入力し、射影座標 $[kx_0, k] = [X_1, Z_1]$ に変換する射影座標変換部と、前記 $[X_1, Z_1]$ から2倍点を演算し出力する2倍演算部と、前記 $[X_1, Z_1]$ から加算点を求め出力する加算演算部と、前記射影座標変換部と前記2倍演算部と前記加算演算部からの情報を得て、座標 x_0 をスカラー倍するスカラー倍部とを有することを特徴とする楕円曲線演算装置。

【請求項7】

楕円曲線が $y^2 + xy = x^3 + ax^2 + b$ である、2の拡大体上の楕円曲線暗号の実行方法を格納した記録媒体であって、前記楕円曲線暗号の実行方法は以下を含む：各座標成分が前記楕円曲線上の点である点 $P_1(x_1, y_1)$ 、 P_2 (

x_2, y_2) の加算を $P_3(x_3, y_3)$ とし、点 $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ の減算を $P_4(x_4, y_4)$ とした場合、前記 x_1 を入力するステップと、前記入力された x_1 を射影空間の X 座標、 Z 座標 $[X_1, Z_1]$ に変換するステップと、前記射影空間の座標 $[X_1, Z_1]$ を記憶するステップと、前記 x_2 を $[X_2, Z_2]$ に変換するステップと、前記 $[X_2, Z_2]$ を記憶するステップと、前記 x_4 を $[X_4, Z_4]$ に変換するステップと、前記 $[X_4, Z_4]$ を記憶するステップと、前記記憶された $[X_1, Z_1]$, $[X_2, Z_2]$, $[X_4, Z_4]$ から $[X_3, Z_3]$ を求めるステップと、前記 $[X_3, Z_3]$ から x_3 に変換するステップと、前記 x_3 を出力するステップとからなり、点 $P_1(x_1, y_1)$ のスカラー倍を計算する。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンピュータネットワークにおいてセキュリティを確保する技術に係り、特に楕円曲線暗号を実行する方法及び装置並びに記録媒体に関する。

【0002】

【従来の技術】

楕円曲線暗号は、V.Miller, N.Koblitz両氏によって、独立に発明された公開鍵暗号である。公開鍵暗号技術において安全上からの要請として、他人に公開される公開鍵から、それに対応する秘密鍵を発見することが事実上不可能であることが求められる。その一方で、秘密鍵暗号方式に比べて基本的に暗号化や復号化に時間のかかる公開鍵暗号方式において、暗号化や復号化におけるより高速のものが求められている状況にある。このように、安全性と高速性という、ある意味で背反的な要請を実現する公開鍵暗号技術として、従来からのRSA暗号やエルガマル暗号に比べてより上述の性質を有する楕円曲線暗号が注目されてきている。

【0003】

楕円曲線暗号は、有限素体上の楕円曲線の標準形 $y^2 = x^3 + ax + b$ ($4a^3 + 27b^2 \neq 0$) や2の拡大体上の楕円曲線の標準形 $y^2 + xy = x^3 + ax$

$^2 + b$ ($b \neq 0$) で表される。この曲線上の点に、無限遠点を加えると、アーベル群が成立する。このアーベル群演算を+記号で表現する。相異なる X, Y 間の演算を $X + Y$ を加算演算と呼ぶ。また、 $X + X$ を2倍演算と呼び、 $2X$ と表現する。

【0004】

かかる楕円曲線は、その計算を容易にするためにアフィン座標における楕円曲線上の点 (X, Y) を射影座標で表現することもある。任意の $\lambda \neq 0$ について、

$[X, Y, Z] = [\lambda^2 X, \lambda^3 Y, \lambda Z]$ となる射影座標を考えると、アフィン座標とこの射影座標の対応は以下で与えられる。すなわち、アフィン座標 (x, y) は、射影座標 $[x, y, 1]$ で表現され、射影座標 $[X, Y, Z]$ は、アフィン座標 $(X/(Z)^2, Y/(Z)^3)$ となる。また、射影座標において $-[X, Y, Z] = [X, -Y, Z]$ である。

【0005】

楕円曲線暗号は、有限体上の楕円曲線を用いて、その有限体となる点の集合を用いる。また、楕円曲線の位数は、楕円曲線の点の数である。以下、 P を s 回加算 ($P + P + \dots + P$) した結果を P の s 倍点といい、これを求める演算を sP と書くと、楕円曲線上の点 P の位数は、 $nP = 0, 1 \leq m < n, mP \neq 0$ となる n である112となる。

【0006】

楕円曲線暗号の鍵は、楕円曲線、ベースポイント、公開鍵、秘密鍵から構成され、具体的には、楕円曲線の係数 a, b 、位数が素数である点 P (ベースポイント)、有限体要素 d (秘密鍵)、ベースポイントの秘密鍵倍の点 Q (公開鍵: $Q = dP$) である。ここで、楕円曲線、ベースポイント、公開鍵は公開情報である。また、公開鍵/秘密鍵は、ユーザ毎に異なる値であり、楕円曲線、ベースポイントは、ユーザ間共通の値である。

【0007】

楕円曲線暗号における、データ暗号化、データ復号化、デジタル署名作成、デジタル署名検証は、任意の点 R のスカラ倍 sR 演算を用いる。これは、上記の加算演算と2倍演算の組合せで、求めることができる。ところが、上記の加算

演算と2倍演算計算法においては、それぞれ1回の除算が必要であり、一般に有限体の除算は非常に時間がかかるため、これを避ける方法が求められる。

【0008】

文献D.V.Chudnovsky, G.V.Chudnovsky "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests", Advances in Applied Mathematics, 7, 385-434, 1986によれば、この有限体の除算を避けるため、射影空間で、加算演算、2倍演算の式を導出している。この場合、素体乗算と、素体加減算では素体乗算が通常、遥かに時間がかかるため、素体乗算演算数で、計算時間を評価できる。この場合、加算演算で、素体乗算(2乗算を含む)が16回必要である。2倍演算において、10回必要である、と述べている。また、楕円曲線の係数 a においても、 $a = -3$ の場合、8回の乗算剰余演算となるとしている。

【0009】

また、P.Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization", Mathematics of computation Vol.48, No.177, pp.243-264 (1987)によれば、有限素体上の楕円曲線の標準形 $By^2 = x^3 + Ax^2 + Bx$ を用いて、点 $P_0(x_0, y_0)$, $P_1(x_1, y_1)$ の加算を $P_3(x_3, y_3)$ 、減算を $P_4(x_4, y_4)$ 、すなわち $P_1 + P_0 = P_3$ 、 $P_1 - P_0 = P_4$ とするとき、 x_0, x_1, x_4 から、 x_3 が高速に求まる。具体的には、素体の乗算6回で求まるとされている。また、 P_1 の2倍点を $P_5(x_5, y_5)$ とするとき、 x_5 は、 x_1 のみから求まり、乗算5回である。これを利用して、点 R のスカラー倍(スカラー値 d) の x 座標を以下のように Rx から求めることができる。

【0010】

初期値を $[R, 2R]$ 、 mR を R の m 倍の x 座標とするとき、 d を2進数展開し、 d の上位ビットから、0の場合は、 $[mR, (m+1)R] \rightarrow [2mR, (2m+1)R]$ となり、1の場合は、 $[mR, (m+1)R] \rightarrow [(2m+1)R, 2(m+1)R]$ となる。尚、 $(m+1)R - mR = R$ 、 $(m+1)R + mR = (2m+1)R$ である。

【0011】

従って、1ビットあたり、 $6 + 5 = 10$ 回の素体乗算（2乗算を含む）でスカラー倍 sP を求めることができる。これを以下、モンゴメリ法と呼ぶ。

【0012】

一方、2の拡大体上の楕円曲線の標準形 $y^2 + xy = x^3 + ax^2 + b$ ($b \neq 0$)で表される。このスカラー倍演算も、加算演算、2倍演算の組合せで実現できる。IEEE P1363 / D2 Standard Specification for Public Key Cryptography (1998)では、加算演算と2倍演算規則を与えている。2の拡大体演算では、2乗算、加減算は相異なる乗算に比べて非常に速く演算できるので、（相異なる）乗算回数で評価できる。加算演算で15回の乗算、2倍演算で5回の乗算が必要となる。しかし、2の拡大体楕円曲線暗号ではモンゴメリ法を用いる演算は知られていない。

【0013】

安全な楕円曲線とするためには、楕円曲線の位数 $\#E(F_q)$ が大きな素因数 r を持つパラメタ a, b を設定する必要がある。 $\#E(F_q) = kr$ で、 k は小さな整数、 r は大きな素数となる。そのが位数大きな素因数を持つ楕円曲線のパラメタの設定方法は、例えば文献Henri Cohen, "A Course in Computational Algebraic Number Theory", GTM138, Springer(1993) p.464 Atkin's Testで記述されている方法がある。

【0014】

次に暗号の攻撃と防御について述べる。近年、暗号の攻撃は、理論的な暗号解読に加え、消費電流波形を統計的に処理して解読を試みるDPA(Differential Power Analysis)や暗号処理時間の違いから統計的に分析し解読を試みるタイミング攻撃等、リーク情報を分析する攻撃とその防御が研究されはじめている。これらの防御研究の多くは、主にICカードを分析する等のハードウェア回路そのものに防御機能を組み込むことが中心になっている。

【0015】

【発明が解決しようとする課題】

上述したように2の拡大体の楕円曲線暗号ではモンゴメリ法を用いる演算は知

られていない。また、楕円曲線暗号の研究においては、主に高速な実行方法、暗号解読の観点からの安全な楕円曲線生成の研究開発が中心であり、リーク情報分析型のアタックに対する防御開発は行われていない。楕円曲線暗号のデータ復号化処理では、与えられた楕円曲線上の点 (x, y) の秘密鍵 d から、 (x, y) の d 倍演算 $d(x, y)$ を行う。 d の偏差情報を消費電流波形や暗号処理時間に洩れる場合 DPA や タイミングアタック への手がかりを与えてしまう。本発明の第 1 の目的は、楕円曲線が $y^2 + xy = x^3 + ax^2 + b$ ($b \neq 0$) である、2 の拡大体上の楕円曲線暗号を高速に演算する方法及び装置を提供することにある。また、本発明の第 2 の目的は、楕円曲線暗号においてタイミングアタックや DPA による攻撃を防御するための、処理時間の偏差情報から秘密鍵情報がもれない方法を提供することにある。

【0016】

【課題を解決するための手段】

本発明の第 1 の目的は、楕円曲線が $y^2 + xy = x^3 + ax^2 + b$ ($b \neq 0$) である、2 の拡大体上の楕円曲線暗号の実行方法であって、各座標成分が前記楕円曲線上の点である点 $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ の加算を $P_3(x_3, y_3)$ とし、点 $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ の減算を $P_4(x_4, y_4)$ とした場合、前記 x_1 を入力するステップと、前記入力された x_1 を射影空間の X 座標、 Z 座標 $[X_1, Z_1]$ に変換するステップと、前記射影空間の座標 $[X_1, Z_1]$ を記憶するステップと、前記 x_2 を $[X_2, Z_2]$ に変換するステップと、前記 $[X_2, Z_2]$ を記憶するステップと、前記 x_4 を $[X_4, Z_4]$ に変換するステップと、前記 $[X_4, Z_4]$ を記憶するステップと、前記記憶された $[X_1, Z_1]$, $[X_2, Z_2]$, $[X_4, Z_4]$ から $[X_3, Z_3]$ を求めるステップと、前記 $[X_3, Z_3]$ から x_3 に変換するステップと、前記 x_3 を出力するステップとからなり、点 $P_1(x_1, y_1)$ のスカラー倍を計算することにより達成される。また、記憶された $[X_1, Z_1]$, $[X_2, Z_2]$, $[X_4, Z_4]$ から x_3 に変換できる $[X_3, Z_3]$ を求めるステップには、 $B = X_1 Z_2^2 + X_2 Z_1^2$ を計算するステップと、前記計算された B を記憶するステップと、前記記憶された B を $B = 0$ であるか否かを判別するス

テップと、 $B=0$ の場合は無限遠点を出力し、 $B \neq 0$ でない場合は $Z_3 = Z_4 B$ を計算するステップと、前記計算された Z_3 を記憶するステップと、前記記憶された Z_3 から $X_3 = X_4 Z_3^2 + X_1 X_2 Z_1^2 Z_2^2 Z_4^2$ を計算するステップとを有することにより達成される。

【0017】

本発明の第2の目的は、2の拡大体上の楕円曲線暗号の復号化処理時間において、処理時間の偏差情報から秘密鍵情報がもれない方法、すなわち楕円曲線が $y^2 + xy = x^3 + ax^2 + b$ である、2の拡大体上の楕円曲線暗号の実行方法であって、各座標成分が前記楕円曲線上の点である点 $P_1(x_1, y_1)$ 、 $P_2(x_2, y_2)$ の加算を $P_3(x_3, y_3)$ とし、点 $P_1(x_1, y_1)$ 、 $P_2(x_2, y_2)$ の減算を $P_4(x_4, y_4)$ とした場合、前記 x_1 を入力するステップと、前記入力された x_1 を射影空間の X 座標、 Z 座標 $[X_1, Z_1]$ に変換するステップと、前記射影空間の座標 $[X_1, Z_1]$ を記憶するステップと、前記 x_2 を $[X_2, Z_2]$ に変換するステップと、前記 $[X_2, Z_2]$ を記憶するステップと、前記 x_4 を $[X_4, Z_4]$ に変換するステップと、前記 $[X_4, Z_4]$ を記憶するステップと、前記記憶された $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ から $[X_3, Z_3]$ を求めるステップと、前記 $[X_3, Z_3]$ から x_3 に変換するステップと、前記 x_3 を出力するステップの他、さらに乱数 k を生成するステップと、前記生成された乱数 k を記憶するステップと、 x 座標を射影座標に変換した後、射影空間の各座標成分と前記記憶された乱数 k と演算させて、射影座標 $[k^2 x, k]$ に変換するステップとを有することにより達成される。すなわち、2の拡大体の演算対象が乱数によって常に変更する方法を用いる。

【0018】

また、乱数 k を生成するステップと、前記生成された乱数 k を記憶するステップと、 x 座標を射影座標に変換した後、射影空間の各座標成分と前記記憶された乱数 k と演算させて、射影座標 $[kx, k]$ に変換するステップとを有することにより達成される。また、楕円曲線が $y^2 + xy = x^3 + ax^2 + b$ である、2の拡大体上の楕円曲線暗号の演算装置であって、乱数 k を生成する乱数生成部と

、2の拡大体上の座標 x_0 と前記乱数 k とを入力し、射影座標 $[k x_0, k] = [X_1, Z_1]$ に変換する射影座標変換部と、前記 $[X_1, Z_1]$ から2倍点を演算し出力する2倍演算部と、前記 $[X_1, Z_1]$ から加算点を求め出力する加算演算部と、前記射影座標変換部と前記2倍演算部と前記加算演算部からの情報を得て、座標 x_0 をスカラー倍するスカラー倍部とを有することにより達成される。

【0019】

また、楕円曲線が $y^2 + xy = x^3 + ax^2 + b$ である、2の拡大体上の楕円曲線暗号の実行方法を格納した記録媒体であって、前記楕円曲線暗号の実行方法は以下を含むことにより達成される。すなわち、各座標成分が前記楕円曲線上の点である点 $P_1(x_1, y_1)$ 、 $P_2(x_2, y_2)$ の加算を $P_3(x_3, y_3)$ とし、点 $P_1(x_1, y_1)$ 、 $P_2(x_2, y_2)$ の減算を $P_4(x_4, y_4)$ とした場合、前記 x_1 を入力するステップと、前記入力された x_1 を射影空間の X 座標、 Z 座標 $[X_1, Z_1]$ に変換するステップと、前記射影空間の座標 $[X_1, Z_1]$ を記憶するステップと、前記 x_2 を $[X_2, Z_2]$ に変換するステップと、前記 $[X_2, Z_2]$ を記憶するステップと、前記 x_4 を $[X_4, Z_4]$ に変換するステップと、前記 $[X_4, Z_4]$ を記憶するステップと、前記記憶された $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ から $[X_3, Z_3]$ を求めるステップと、前記 $[X_3, Z_3]$ から x_3 に変換するステップと、前記 x_3 を出力するステップとからなり、点 $P_1(x_1, y_1)$ のスカラー倍を計算する。

【0020】

また、上述した2の拡大体上の楕円曲線暗号の実行方法は、素体上の楕円曲線暗号の復号化処理時間において、処理時間の偏差情報から秘密鍵情報がもれない方法としても適用可能である。素体上の楕円曲線暗号において、上記課題(2)を解決するため、次の(a)、(b)を組合わせる。次の(a)、(b)を組合わせる。(a)楕円曲線のスカラー倍 $d(x, y)$ において、素体上の楕円曲線の標準形 $By^2 = x^3 + Ax^2 + Bx$ の場合、モンゴメリのスカラー倍を用いる。(b)スカラー倍 $d(x, y)$ を計算する場合、このアフィン座標 (x, y)

を射影座標する際に、乱数 k を生成し、 $(x, y) \rightarrow [kx, ky, k]$ または $(x, y) \rightarrow [k^2x, k^3y, k]$ に変換する。このことにより、素体の演算対象が乱数によって常に変更する方法を用いる。

【0021】

【発明の実施の形態】

2の拡大体上の楕円曲線の標準形 $y^2 + xy = x^3 + ax^2 + b$ ($b \neq 0$) のアフィン座標における演算規則を以下に示す。

【0022】

- 1) $0 + 0 = 0$
- 2) $(x, y) + 0 = (x, y)$
- 3) $(x, y) + (x, x+y) = 0$
- 4) 可換性 $(x_0, y_0) + (x_1, y_1) = (x_1, y_1) + (x_0, y_0)$

- 5) 加算演算 $(x_2, y_2) = (x_1, y_1) + (x_0, y_0)$
 $x_2 = a + \lambda^2 + \lambda + x_0 + x_1$; $y_2 = \lambda(x_1 + x_2) + x_2 + y_1$;

$$\lambda = (y_0 + y_1) / (x_0 + x_1)$$

- 6) 2倍演算 $(x_2, y_2) = (x_1, y_1) + (x_1, y_1) = 2(x_1, y_1)$

$$x_2 = a + \lambda^2 + \lambda$$
; $y_2 = \lambda(x_1 + x_2) + x_2 + y_1$; $\lambda = x_1 + (y_1 / x_1)$

$$\text{または、} x_2 = (x_1)^2 + b / (x_1)^2$$

かかる楕円曲線は、その計算を容易にするためにアフィン座標における楕円曲線上の点 (X, Y) を射影座標で表現することもある。任意の $\lambda \neq 0$ について、 $[X, Y, Z] = [\lambda^2 X, \lambda^3 Y, \lambda Z]$ となる射影座標を考えると、アフィン座標とこの射影座標の対応は以下で与えられる。すなわち、アフィン座標 (x, y) は、射影座標 $[x, y, 1]$ で表現され、射影座標 $[X, Y, Z]$ は、アフィン座標 $(X / (Z)^2, Y / (Z)^3)$ となる。また、射影座標において $[X, Y, Z] = [X, XZ + Y, Z]$ である。

【0023】

以下、本発明の実施例を図面を用いて具体的に説明する。図10は、楕円曲線暗号システムの構成図である。入出力インターフェース1001は暗号化する平文を入力するキーボード等の入力装置、復号化した平文を出力するディスプレイ、プリンタ等の出力装置、平文を記憶するメモリ等の記憶装置などである。暗号化部1002は、楕円曲線生成部1003で生成された楕円曲線と、公開鍵、暗号鍵生成部1004からの鍵とを入力し、平文を暗号化する。ここで、公開鍵、暗号鍵は対になっており、どちらの鍵を暗号化部1002、復号化部1006に与えるかは暗号システムの用途、即ち、秘密通信に用いるか、署名・認証と呼ばれる通信に用いるか等で使い分ける。暗号化された暗号文は接続インターフェース1005から送信される。復号化部1006は、暗号文を復号化し平文にする。

【0024】

図1は、楕円曲線暗号システムにおける処理の流れを示す図である。楕円曲線生成部101では楕円曲線暗号に使用する楕円曲線を生成する。公開鍵／秘密鍵生成部102では、楕円曲線生成部101で生成した楕円曲線を入力し、これに基づいて公開鍵115と秘密鍵116を生成する。暗号化部103では、平文113、公開鍵115、楕円曲線を入力して暗号文112を出力する。復号化部104では、暗号文112、秘密鍵116、楕円曲線を入力し、平文114を出力するが、ここで出力する平文114は平文113と内容が同じものである。

【0025】

楕円曲線生成部101では以下の手順で楕円曲線を生成する。原始多項式(primitive polynomials)設定105では、素体 F_2 上の原始多項式 $f(x)$ を設定する。例えば、素体 F_2 上の原始多項式は、A.Menezes, P.Oorschot, S.Vanstone, "Handbook of Applied Cryptography", CRC Press(1996)の第4.5.3 Primitive polynomialsに記述されている。

【0026】

楕円曲線パラメタ設定106は、 2 の拡大体 F_q を定義体とする楕円曲線 $y^2 + xy = x^3 + ax^2 + b$ のパラメタ a, b を設定する。安全な楕円曲線とする

ためには、楕円曲線の位数 $\#E(Fq)$ が大きな素因数 r を持つ必要がある。 $\#E(Fq) = kr$ の場合、 k を小さな整数とすることによって、 r は大きな素数となる。大きな素因数 r を位数に持つ楕円曲線を生成する方法として、文献 Henri Cohen, "A Course in Computational Algebraic Number Theory", GTM138, Springer(1993) p.464 Atkin's Test で記述されている方法がある。なお、他の楕円曲線の位数が大きな素因数 r を持つ楕円曲線パラメタ設定法を用いても本発明の実施は可能である。

【0027】

ベースポイント生成部 107 は、楕円曲線上のアーベル群において、上記 r を位数とする部分巡回群の生成元を求める。例えば、 $\#E(Fq) = kr$ の場合は、第1のステップで $E(Fq)$ 上の任意の点 (x_1, y_1) を求める。次に第2のステップで $r(x_1, y_1) = 0$ かつ $k(x_1, y_1) \neq 0$ の場合、 $G = (x_1, y_1)$ をベースポイントとする。他の場合は、第1のステップへ戻る。

【0028】

ここで、 $r(x_1, y_1)$ は、 (x_1, y_1) のスカラー倍 (r 倍) 演算を実行するという意味である。スカラー倍 (r 倍) 演算については楕円曲線演算部 109 で説明する。

【0029】

以上、楕円曲線生成部 101 により、原始多項式 $f(x)$ 、楕円曲線 $y^2 + xy = x^3 + ax^2 + b$ のパラメタ a, b 、ベースポイント G 、ベースポイントの位数 r を生成した。これらは公開する情報である。

【0030】

次に公開鍵／秘密鍵生成部 102 は、以下の手順で公開鍵と秘密鍵を生成する。入力を原始多項式 $f(x)$ 、楕円曲線 $y^2 + xy = x^3 + ax^2 + b$ のパラメタ a, b 、ベースポイント G とし、出力を公開鍵 Q 、秘密鍵 d とすると、第1のステップで乱数 $2 < d < r - 1$ を生成し、第2のステップで $Q = dG$ すなわち G のスカラー倍 (d 倍) 点を求める。

【0031】

公開鍵は、公開する情報であり、秘密鍵は秘密にする情報である。 Q, G から

dを求める問題は、離散対数問題といわれるものであり、楕円曲線において、ベースポイントの位数 r のビット長の指数オーダの計算量を必要とする。このため、 r が大きな素数であれば例えば、 $r > 2$ の159乗をとれば、事実上、 Q 、 G から d を求めることはできなくなる。これが楕円曲線暗号の原理である。なお、 Q を計算する方法は、従来技術文献 D.V.Chudnovsky, G.V.Chudnovsky "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests", Advances in Applied Mathematics, 7, 385-434, 1986で記載されている方法で求めることができる。

【0032】

次に、暗号化部103では、以下の手順で平文113を暗号文114に変換する。入力を平文 M 、公開鍵 Q 、原始多項式 $f(x)$ 、楕円曲線 $y^2 + xy = x^3 + ax^2 + b$ のパラメタ b 、ベースポイント G とし、出力を暗号文 C とすると、第1のステップで乱数 k を生成し（乱数生成部108）、第2のステップでベースポイント G と第1のステップで生成した乱数 k とを演算し、 kG すなわち (kx_1, ky_1) とする（楕円曲線演算部109）。第3のステップで公開鍵 Q と第1のステップで生成した乱数 k とを演算し、 kQ すなわち (kx_2, ky_2) とする（楕円曲線演算部109）。第4のステップで $M \oplus x_2$ を演算し、 M' とする（データ暗号化110）。第5のステップで $x_1 || y_1 || M'$ を演算し暗号文 C とする（データ暗号化110）。

【0033】

楕円曲線演算部109は、任意の点 R のスカラ倍 kR 演算を行いその x 座標を得る。これにより2の拡大体上の楕円曲線暗号の復号化処理時間において、処理時間の偏差情報から秘密鍵情報が漏れなくなる。以下にこのスカラ倍方法を説明する。図2、図3は、このスカラ倍方法の第1の実施例の説明図である。

【0034】

＜第1実施例スカラ倍方法＞

R の x 座標の射影座標成分 X_0 、スカラ値 m を入力とし、 R の m 倍の点の x 座標の射影座標成分 X_m を出力とする。 m 、 X_0 を入力を入力し（ステップ202）、ステップ203から205では乱数を射影座標の各座標に乗算することに

より、データを攪拌する。すなわち、乱数 k を生成し（ステップ203）、乱数 k と X_0 を演算して $k^2 X_0$ を X_1 に代入し、乱数 k を Z_1 に代入する（ステップ205）。ステップ206から208及び301ではスカラー倍の準備を行う。すなわち、 $[X_1, Z_1]$ を $[X_4, Z_4]$ に代入し（ステップ206）、また $[X_1, Z_1]$ を2倍方法（図5）に入力し、出力を $[X_2, Z_2]$ へ代入する（ステップ207）。 m の2進数表現を $h_i h_{i-1} \dots h_0$ とする（ステップ208）。ただし、最上位ビット h_1 は1である。 i を1とする（ステップ301）。ステップ302から309では m の1ビットが0か1かによって加算方法や2倍方法を制御しスカラー倍を求める。すなわち、 $i-1$ を i に代入し（ステップ302）、 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ を加算方法（図4）に入力し、出力を $[X_3, Z_3]$ へ代入する（ステップ303）。ここで、 $h_i = 0$ ならば、ステップ304へ、1ならばステップ306へ進む（ステップ304）。 $[X_1, Z_1]$ を2倍方法（図5）に入力し、出力を $[X_1, Z_1]$ に代入する（ステップ305）。 $[X_3, Z_3]$ を $[X_2, Z_2]$ に代入し、ステップ308へいく（ステップ306）。 $[X_2, Z_2]$ を2倍方法（図5）に入力し、出力を $[X_2, Z_2]$ に代入する（ステップ307）。 $[X_3, Z_3]$ を $[X_1, Z_1]$ に代入し、ステップ308へいく（ステップ308）。 $i > 0$ ならばステップ302へ進む（ステップ309）。次は、射影座標から (x, y) 座標の x 座標へ変換する。 $X_1 / (Z_1)^2$ を X_m に代入し（ステップ310）、 X_m を出力する（ステップ311）。

【0035】

次に、加算方法について説明する。楕円曲線上の点の射影空間座標として、任意の $\lambda \neq 0$ について、 $[X, Y, Z] = [\lambda^2 X, \lambda^3 Y, \lambda Z]$ とする。ここで、楕円曲線上の点 $P_0 = (x_0, y_0) = [X_0, Y_0, Z_0]$; $P_1 = (x_1, y_1) = [X_1, Y_1, Z_1]$ とする。この和と差を $P_3 = (x_3, y_3) = [X_3, Y_3, Z_3]$, $P_4 = (x_4, y_4) = [X_4, Y_4, Z_4]$ とする。

【0036】

$P_1 + P_0 = P_3$;

$$P_1 - P_0 = P_4 ;$$

$$x_3 = a + (\lambda_3)^2 + \lambda_3 + x_0 + x_1 ; \lambda_3 = (y_0 + y_1) / (x_0 + x_1) ;$$

$$x_4 = a + (\lambda_4)^2 + \lambda_4 + x_0 + x_1 ; \lambda_4 = (x_0 + y_0 + y_1) / (x_0 + x_1) ;$$

$$\lambda_3 + \lambda_4 = (x_0) / (x_0 + x_1) ;$$

$$(\lambda_3)^2 + (\lambda_4)^2 = (x_0)^2 / (x_0 + x_1)^2 ;$$

$$x_3 + x_4 = ((x_0)^2 + (x_0)(x_0 + x_1)) / (x_0 + x_1)^2 = (x_0 x_1) / (x_0 + x_1)^2 ;$$

$$\text{以上により、} x_3 + x_4 = (x_0 x_1) / (x_0 + x_1)^2 \text{ ----- (1)}$$

という関係式が得られた。

【0037】

次に、射影座標での関係式を導出する。

【0038】

$x_1 = X_1 / (Z_1)^2$ 、 $x_0 = X_0 / (Z_0)^2$ を(1)式に代入する。

$$X_3 / (Z_3)^2 = X_4 / (Z_4)^2 + ((X_0 / (Z_0)^2) (X_1 / (Z_1)^2)) / (X_0 / (Z_0)^2 + X_1 / (Z_1)^2)^2 ;$$

$$= X_4 / (Z_4)^2 + ((X_0 (Z_0)^2) (X_1 (Z_1)^2)) / (X_0 (Z_1)^2 + X_1 (Z_0)^2)^2 ;$$

$$= ((X_4 \beta^2) + Z_4^2 (X_0 Z_0^2) (X_1 Z_1^2))$$

$$/ (Z_4^2 \beta^2)$$

$$\text{ただし、} \beta = X_0 Z_1^2 + X_1 Z_0^2$$

これより、

$$X_3 = X_4 \beta^2 + Z_4^2 (X_0 Z_1^2) (X_1 Z_0^2) ; \text{----- (2)}$$

)

$$Z_3 = Z_4 \beta ; \text{----- (3) を}$$

得た。

【0039】

ここで、 $mR = [X_1, Y_1, Z_1]$ 、 $(m+1)R = [X_2, Y_2, Z_2]$ 、 $R = [X_4, Y_4, Z_4]$ 、 $(2m+1)R = [X_3, Y_3, Z_3]$ とする。

この導出式を利用した加算方法を以下に説明する。図4はこの方法の説明図であ

る。

【0040】

<第1実施例加算方法>

射影座標 $[X_1, Z_1]$, $[X_2, Z_2]$, $[X_4, Z_4]$ を入力とし、 $[X_3, Z_3]$ または無限遠点を出力とする。 $[X_1, Z_1]$, $[X_2, Z_2]$, $[X_4, Z_4]$ を入力し (ステップ402)、ステップ403から407では加算結果が無限遠点か判定するために $X_1 (Z_2)^2 + X_2 (Z_1)^2$ を求める。さらに各中間結果 S_1 、 S_2 、 B は、上記式 (2)、(3) を求めるための準備である。すなわち、 $X_1 (Z_2)^2$ を S_1 に代入し (ステップ403)、 $X_2 (Z_1)^2$ を S_2 に代入し (ステップ404)、 $S_1 + S_2$ を B に代入し (ステップ405)、 $B = 0$ の場合、ステップ407へ進み、成立しない場合ステップ408へ進む (ステップ406)。ステップ407では、無限遠点を出力し、ステップ413へいく。以下の408-411は上記式 (2)、(3) に従って $[X_3, Z_3]$ を求める。 $Z_4 B$ を Z_3 に代入し (ステップ408)、 $(Z_4)^2 S_1 S_2$ を S に代入し (ステップ409)、 $X_4 Z_3^2$ を M に代入し (ステップ410)、 $M + S$ を X_3 に代入し (ステップ411)、 $[X_3, Z_3]$ を出力を出力する (ステップ412)。かかる方法により相異なる変数の乗算6回で加算演算を実行できる。すなわち、 X_1 、 X_2 、 X_4 から X_3 を高速に演算できる。

【0041】

次に、2倍計算方法について説明する。 $P1$ の2倍点を $P2$ とし、 $P1 = (x_1, y_1) = [X_1, Y_1, Z_1]$ 、 $P2 = (x_2, y_2) = [X_2, Y_2, Z_2]$ とする。2倍演算の演算式 $x_2 = (x_1)^2 + b / (x_1)^2$ より、 $x_1 = X_1 / (Z_1)^2$ 、 $x_2 = X_2 / (Z_2)^2$ をこの式に代入する。

【0042】

$$X_2 / (Z_2)^2 = (X_1 / (Z_1)^2)^2 + b / (X_1 / (Z_1)^2)^2 = X_1^2 / (Z_1)^4 + (b (Z_1)^4) / (X_1)^2 = (X_1^4 + b (Z_1)^8) / (X_1^2 Z_1^4)$$

従って、

$$X_2 = X_1^4 + b Z_1^8 \text{ ----- (4)}$$

$$Z_2 = X_1 Z_1^2 \text{ ----- (5)}$$

この導出式を利用した2倍方法を以下に説明する。図5は、この説明図である。

【0043】

＜第1実施例2倍計算方法＞

$Q = [X_1, Z_1]$ 、 b を入力とし、 $2Q = [X_2, Z_2]$ または無限遠点を出力とする。 X_1, Z_1 を入力し（ステップ502）、以下のステップ503から504は2倍結果が無限遠点を判定するために $X_1 = 0$ または $Z_1 = 0$ の判定を行う。すなわち、 $X_1 = 0$ または $Z_1 = 0$ の場合は、ステップ504へ。成立しない場合は、ステップ505へいく（ステップ503）。ステップ504では、無限遠点を出力する。以下のステップ505から507では上記式（4）、（5）に従って $[X_2, Z_2]$ を求める。 Z_1^2 を S に代入し（ステップ505）、 $X_1 S$ を Z_2 に代入し（ステップ506）、 $X_1^4 + b(S)^4$ を X_2 に代入し（ステップ507）、 $[X_2, Z_2]$ を出力する（ステップ508）。かかる方法により相異なる変数の乗算2回で加算演算を実行できる。従って、＜スカラー倍方法＞においてはスカラー値 d のビットあたり、相異なる変数の乗算 $6 + 2 = 8$ 回で実行できる。すなわち、 X_1, X_2, X_4 から X_3 を高速に演算できる。

【0044】

つぎに、復号化部104では、以下の手順で暗号文112を元の平文114に変換する。112と114は内容が同じ平文である。入力を暗号文 $C \leftarrow x_1 || y_1 || M'$ 、秘密鍵 d 、原始多項式 $f(x)$ 、楕円曲線 $y^2 + xy = x^3 + ax^2 + b$ のパラメタ、 b 、ベースポイント G とし、出力を平文 M とする。

【0045】

ステップ1： $(x_2, y_2) \leftarrow d(x_1, y_1)$ （楕円曲線演算部111）

ステップ2：平文 $M \leftarrow M' \oplus x_2$

ステップ1は図2、図3を用いて実行する。

【0046】

以上により、与えられた座標 (x, y) の d スカラー倍の x 座標を求める処理

において、 d のビットパターンに依存せず、 d の各ビットあたり8回の相異なる乗算処理で実現することができる。また、 d の与えられた x 座標に対して、乱数 k により $[kx^2, k]$ をスカラー倍初期値とすることによって、常に演算対象を変動させることができる。さらに、これらの組合わせにより、 d のビットパターンが、 $d(x, y)$ 処理時間の偏差に現れないため、 $d(x, y)$ 処理時間の偏差情報から秘密鍵情報がもれない方法を示した。また、この性質は暗号処理の電流、電圧、電力の偏差を用いて、暗号解読を行うDPA(Differential Power Analysis)に対して、 $d(x, y)$ の処理電流(電圧、電力)の偏差情報から秘密鍵情報がもれない方法をも示している。

【0047】

次に第1実施例を更に高速化を図ることが可能な第2実施例を説明する。アフィン座標から、射影座標への変換を $(x, y) \rightarrow [x, y, 1]$ とする場合、 $Z_4 = 1$ とできる。(2)、(3)式に $Z_4 = 1$ を代入すると、

$$X_3 = (X_4 \beta^2) + (X_0(Z_1)^2)(X_0(Z_1)^2) \text{ ----- (6)}$$

$$Z_3 = \beta \text{ ----- (7)}$$

この式を利用してスカラー倍方法、加算方法を以下のように求めることができる。

【0048】

<第2実施例スカラー倍方法>

これを図6、図7に示す。 R の x 座標の射影座標成分 X_0 、スカラー値 m を入力とし、 R の m 倍の点の x 座標の射影座標成分 X_m を出力とする。 m, X_0 を入力し(ステップ602)、以下のステップ603から604では X_0 を射影座標に変換する。 X_0 を X_1 に代入し(ステップ603)、1を Z_1 に代入する(ステップ604)。ステップ605から607ではスカラー倍の準備を行う。すなわち、 $[X_1, Z_1]$ を $[X_4, Z_4]$ に代入し(ステップ605)、 $[X_1, Z_1]$ を2倍方法(図5)に入力し、出力を $[X_2, Z_2]$ へ代入する(ステップ606)。 m の2進数表現を $h_i h_{i-1} \dots h_0$ とする(ステップ607)。ただし、最上位ビット h_i は1である。1を i に代入する(ステップ701)。以下のステップ702から709では m の1ビットが0か1かによって加

算方法や2倍方法を制御しスカラー倍を求める。すなわち、 $i-1$ を i に代入し（ステップ702）、 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 X_0 を加算方法（図8）に入力し、出力を $[X_3, Z_3]$ へ代入する（ステップ703）。 $h_i = 0$ ならば、ステップ706へ、1ならばステップ708へ進む（ステップ704）。 $[X_1, Z_1]$ を2倍方法（図5）に入力し、出力を $[X_1, Z_1]$ に代入する（ステップ705）。 $[X_3, Z_3]$ を $[X_2, Z_2]$ に代入し、ステップ710へいく（ステップ706）。 $[X_2, Z_2]$ を2倍方法（図5）に入力し、出力を $[X_2, Z_2]$ に代入する（ステップ707）。 $[X_3, Z_3]$ を $[X_1, Z_1]$ へ代入し、ステップ710へいく（ステップ708）。 $i > 0$ ならばステップ703へ進む（ステップ709）。 $X_1 / (Z_1)^2$ を X_m に代入し（ステップ710）、 X_m を出力する（ステップ711）。

【0049】

＜第2実施例加算方法＞

これを図8に示す。 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 X_4 を入力とし、 $[X_3, Z_3]$ または無限遠点を出力とする。 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 X_4 を入力し（ステップ802）、以下のステップ803から807は加算結果が無限遠点か判定するために $X_1 (Z_2)^2 + X_2 (Z_1)^2$ を求める。さらに各中間結果 S_1 、 S_2 、 B は、上記式（6）、（7）を求めるための準備である。すなわち、 $X_1 Z_2^2$ を S_1 に代入し（ステップ803）、 $X_2 Z_1^2$ を S_2 に代入し（ステップ804）、 $S_1 + S_2$ を B に代入する（ステップ805）。 $B = 0$ の場合は、ステップ807へ進み、成立しない場合ステップ808へ進む（ステップ806）。無限遠点を出力し、ステップ813へいく（ステップ807）。以下のステップ808から811は上記式（6）、（7）に従って $[X_3, Z_3]$ を求める。すなわち、 B を Z_3 に代入し（ステップ808）、 $S_1 S_2$ を S に代入し（ステップ809）、 $X_4 Z_3^2$ を M に代入し（ステップ810）、 $M + S$ を X_3 に代入し（ステップ811）、 $[X_3, Z_3]$ を出力する（ステップ812）。

【0050】

以上により、相異なる変数の乗算4回で加算演算を実行できる。このため、第

1 実施例の加算演算より、乗算回数を減らすことができる。なお、2倍演算は第1実施例の2倍演算を利用する。

【0051】

上述した処理時間の偏差情報から秘密鍵情報が漏れない方法は、2の拡大体上の楕円曲線の場合の他、素体上の楕円曲線でも適用可能である。

【0052】

次に第3実施例を説明する。素体上の楕円曲線 $By^2 = x^3 + Ax^2 + Bx$ の場合、モンゴメリ法を用いて、処理時間の偏差情報から秘密鍵情報がもれない方法を示す。

【0053】

P.Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization", Mathematics of computation Vol.48, No.177, pp.243-264(1987)では、有限素体上の楕円曲線の標準形 $By^2 = x^3 + Ax^2 + Bx$ を用いて、点 $P_0(x_0, y_0)$, $P_1(x_1, y_1)$ の加算と、減算を

$$P_3(x_3, y_3); P_4(x_4, y_4);$$

$$P_1 + P_0 = P_3;$$

$$P_1 - P_0 = P_4; \text{ とするとき、}$$

x_0, x_1, x_4 から、 x_3 が高速に求まる。具体的には、次のように素体の乗算6回で求まる。

【0054】

$$(x_3, y_3) \rightarrow [X_3, Z_3]; (x_4, y_4) \rightarrow [X_4, Z_4];$$

とするとき、

$$X_3 \leftarrow Z_4 [(X_1 - Z_1)(X_0 + Z_0) + (X_1 + Z_1)(X_0 - Z_0)]^2;$$

$$Z_3 \leftarrow X_4 [(X_1 - Z_1)(X_0 + Z_0) - (X_1 + Z_1)(X_0 - Z_0)]^2;$$

また、2倍演算は、

$$P_5 = 2P_1; (x_1, y_1) \rightarrow [X_1, Z_1];$$

$$4X_1Z_1 \leftarrow (X_1 + Z_1)^2 - (X_1 - Z_1)^2;$$

$$X_5 \leftarrow (X_1 + Z_1)^2 (X_1 - Z_1)^2; Z_5 \leftarrow (4X_1 Z_1) [(X_1 - Z_1)^2 + ((A+2)/4)(4X_1 Z_1)] ;$$

また、P1の2倍点P5 (x5, y5) とするとき、x5は、x1のみから求まり、乗算5回である。これを利用して、点Rのスカラー倍（スカラー値d）のx座標を以下のようにRxから求める。

【0055】

初期値を[R, 2R]、mRをRのm倍のx座標とするとき、dを2進数展開し、dの上位ビットから、

$$0 \text{ の場合、 } [mR, (m+1)R] \rightarrow [2mR, (2m+1)R]$$

$$1 \text{ の場合、 } [mR, (m+1)R] \rightarrow [(2m+1)R, 2(m+1)R]$$

$$(m+1)R - mR = R$$

$$(m+1)R + mR = (2m+1)R \text{ である。}$$

【0056】

<第3実施例スカラー倍方法>

Rのx座標の射影座標成分 X_0 、スカラー値mを入力とし、Rのm倍の点のx座標の射影座標成分 X_m を出力とする。m, X_0 を入力を入力し（ステップ902）、ステップ903から905では乱数を射影座標の各座標に乗算することにより、データを攪拌する。すなわち、乱数kを生成し（ステップ903）、乱数kと X_0 を演算して kX_0 を X_1 に代入し（ステップ904）、乱数kを Z_1 に代入する（ステップ905）。次に、 $[X_1, Z_1]$ を $[X_4, Z_4]$ に代入し（ステップ906）、 $[X_1, Z_1]$ を2倍方法（モンゴメリの2倍演算）に入力し、出力を $[X_2, Z_2]$ へ代入する（ステップ907）。mの2進数表現を $h_i h_{i-1} \dots h_0$ とする（ステップ908）。ただし、最上位ビット h_1 は1である。iを1とする（ステップ909）。i-1をiに代入し（ステップ910）、 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ を加算方法（モンゴメリの加算演算）に入力し、出力を $[X_3, Z_3]$ へ代入する（ステップ911）。ここで、 $h_i = 0$ ならば、ステップ912へ、1ならばステップ914へ進む（ステップ912）。 $[X_1, Z_1]$ を2倍方法（モンゴメリの2倍演算）に入力し、出力を $[X_1, Z_1]$ に代入する（ステップ913）。 $[X_3, Z_3]$ を $[X_2, Z_2]$ に代入し、ステップ916へいく（ステップ914）

。 $[X_2, Z_2]$ を 2 倍方法 (モンゴメリの 2 倍演算) に入力し、出力を $[X_2, Z_2]$ に代入する (ステップ 915)。 $[X_3, Z_3]$ を $[X_1, Z_1]$ に代入し、ステップ 916 へいく (ステップ 916)。 $i > 0$ ならばステップ 910 へ進む (ステップ 917)。 X_1 / Z_1 を X_m に代入し (ステップ 918)、 X_m を出力する (ステップ 919)。

【0057】

以上により、与えられた座標 (x, y) の d スカラー倍の x 座標を求める処理において、 d の各ビットあたり 11 回の相異なる乗算処理で実現し、与えられた x 座標に対して、乱数 k により $[kx, k]$ をスカラー倍初期値とすることによって、 $d(x, y)$ 処理時間の偏差情報から秘密鍵情報がもれない方法を示した。また、この性質は暗号処理の電流、電圧、電力の偏差を用いて、暗号解読を行う DPA に対して、 $d(x, y)$ の処理電流 (電圧、電力) の偏差情報から秘密鍵情報がもれない方法を示している。

【0058】

さらに、素体上の楕円曲線 $y^2 = x^3 + ax + b$ の場合、 $By^2 = x^3 + Ax^2 + Bx$ と $y^2 = x^3 + ax + b$ の間に有理点がなすアーベル群が同型となる楕円曲線を構成し、素体上の楕円曲線 $y^2 = x^3 + ax + b$ で与えられた (x, y) を $By^2 = x^3 + Ax^2 + Bx$ に変換し、上記発明の方法でスカラー倍を求め、結果を $y^2 = x^3 + ax + b$ に変換することにより本発明を利用することができる。

【0059】

次に第 4 実施例を説明する。第 1 実施例では、射影座標を任意の $\lambda \neq 0$ について、 $[X, Y, Z] = [\lambda^2 X, \lambda^3 Y, \lambda Z]$ とするものを説明したが、 $[X, Y, Z] = [\lambda X, \lambda Y, \lambda Z]$ とする射影座標で実施することもできる。

【0060】

<第 4 実施例スカラー倍方法>

R の x 座標の射影座標成分 X_0 、スカラー値 m を入力とし、 R の m 倍の点の x 座標の射影座標成分 X_m を出力とする。 m, X_0 を入力し (ステップ 1002)、以下のステップ 1003 から 1005 では乱数を射影座標の各座標に乗算する

ことにより、データを攪拌する。すなわち、乱数 k を生成し（ステップ1003）、 kX_0 を X_1 に代入し（ステップ1004）、乱数 k を Z_1 に代入する（ステップ1005）。 $[X_1, Z_1]$ を $[X_4, Z_4]$ に代入し（ステップ1006）、 $[X_1, Z_1]$ を2倍方法に入力し、出力を $[X_2, Z_2]$ へ代入する（ステップ1007）。 m の2進数表現を $h_i h_{i-1} \dots h_0$ とする（ステップ1008）。ただし、最上位ビット h_1 は1である。 i を1とする（ステップ1009）。 $i-1$ を i に代入し（ステップ1010）、 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ を加算方法に入力し、出力を $[X_3, Z_3]$ へ代入する（ステップ1011）。ここで、 $h_i = 0$ ならば、ステップ1012へ、1ならばステップ1014へ進む（ステップ1012）。 $[X_1, Z_1]$ を2倍方法に入力し、出力を $[X_1, Z_1]$ に代入する（ステップ1013）。 $[X_3, Z_3]$ を $[X_2, Z_2]$ に代入し、ステップ1016へいく（ステップ1014）。 $[X_2, Z_2]$ を2倍方法に入力し、出力を $[X_2, Z_2]$ に代入する（ステップ1015）。 $[X_3, Z_3]$ を $[X_1, Z_1]$ に代入し、ステップ1016へいく（ステップ1016）。 $i > 0$ ならばステップ1010へ進む（ステップ1017）。 X_1/Z_1 を X_m に代入し（ステップ1018）、 X_m を出力する（ステップ1019）。

【0061】

楕円曲線上の点の射影空間座標として、任意の $\lambda \neq 0$ について、 $[X, Y, Z] = [\lambda X, \lambda Y, \lambda Z]$ とする。ここで、楕円曲線上の点 $P0 = (x0, y0) = [X0, Y0, Z0]$ ； $P1 = (x1, y1) = [X1, Y1, Z1]$ とする。この和と差を $P3 = (x3, y3) = [X3, Y3, Z3]$ ， $P4 = (x4, y4) = [X4, Y4, Z4]$ とする。

【0062】

$$P1 + P0 = P3 ;$$

$$P1 - P0 = P4 ;$$

第1実施例の(1)式 $x3 + x4 = (x0x1) / (x0 + x1)^2$ より射影座標での関係式を導出する。

【0063】

$x_1 = X_1 / Z_1$ 、 $x_0 = X_0 / Z_0$ を(1)式に代入する。

$$\begin{aligned} X_3 / Z_3 &= X_4 / Z_4 + ((X_0 / Z_0) (X_1 / Z_1)) / (X_0 / Z_0 + X_1 / Z_1)^2; \\ &= X_4 / (Z_4)^2 + ((X_0 Z_0) (X_1 Z_1)) / (X_0 Z_1 + X_1 Z_0)^2; \\ &= ((X_4 \beta^2) + Z_4^2 (X_0 Z_0) (X_1 Z_1)) / (Z_4^2 \beta^2) \end{aligned}$$

ただし、 $\beta = X_0 Z_1 + X_1 Z_0$

これより、 $X_3 = (X_4 \beta^2) + Z_4^2 (X_0 Z_1) (X_1 Z_0)$ ；
- (2)'

$$Z_3 = Z_4^2 \beta^2 ; \text{-----} (3)$$

を得た。

【0064】

ここで、 $mR = [X_1, Y_1, Z_1]$ 、 $(m+1)R = [X_2, Y_2, Z_2]$ 、 $R = [X_4, Y_4, Z_4]$ 、 $(2m+1)R = [X_3, Y_3, Z_3]$ とする。
この導出式を利用した加算方法を以下に説明する。

【0065】

<第4実施例加算方法>

射影座標 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ を入力とし、 $[X_3, Z_3]$ または無限遠点を出力とする。 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ を入力し(ステップ1102)、 $X_1 Z_2$ を S_1 に代入し(ステップ1103)、 $X_2 Z_1$ を S_2 に代入し(ステップ1104)、 $S_1 + S_2$ を B に代入する(ステップ1105)。 $B=0$ の場合は、ステップ1107へ進み、成立しない場合ステップ1108へ進む(ステップ1106)。無限遠点を出力し、ステップ1113へいく(ステップ1107)。 $(Z_4)^2 B^2$ を Z_3 に代入し(ステップ1108)、 $(Z_4)^2 S_1 S_2$ を S に代入し(ステップ1109)、 $(X_4 B^2)$ を M に代入し(ステップ1110)、 $M+S$ を X_3 に代入し(ステップ1111)、 $[X_3, Z_3]$ を出力する(ステップ1111)

2)。

【0066】

以上により、相異なる変数の乗算6回で加算演算を実行できる。

【0067】

次に、2倍計算方法について説明する。P1の2倍点をP2とし、 $P1 = (x_1, y_1) = [X_1, Y_1, Z_1]$ 、 $P2 = (x_2, y_2) = [X_2, Y_2, Z_2]$ とする。2倍演算の演算式 $x_2 = (x_1)^2 + b / (x_1)^2$ より、 $x_1 = X_1 / Z_1$ 、 $x_2 = X_2 / Z_2$ をこの式に代入する。

【0068】

$$X_2/Z_2 = (X_1/Z_1)^2 + b / (X_1/Z_1)^2 = X_1^2 / (Z_1)^2 + (bZ_1^2) / (X_1)^2 = (X_1^4 + bZ_1^4) / (X_1^2 Z_1^2)$$

従って、

$$X_2 = X_1^4 + bZ_1^4 \text{ ----- (4) '}$$

$$Z_2 = X_1^2 Z_1^2 \text{ ----- (5) '}$$

この導出式を利用した2倍方法を以下に説明する。

【0069】

<第4実施例2倍計算方法>

$Q = [X_1, Z_1]$ 、 b を入力とし、 $2Q = [X_2, Z_2]$ または無限遠点を出力する。 X_1, Z_1 を入力し(ステップ1202)、 $X_2 = 0$ または $Z_2 = 0$ の場合、ステップ1204へ。成立しない場合、ステップ1205へいく(ステップ1203)。ステップ1204では、無限遠点を出力する。 $Z_2 = X_1^2 Z_1^2$ とし(ステップ1205)、 $S = bZ_1^4$ とし(ステップ1206)、 $X_1^4 + S$ を X_2 に代入し(ステップ1207)、 $[X_2, Z_2]$ を出力する(ステップ1208)。かかる方法により、相異なる変数の乗算2回で加算演算を実行できる。

【0070】

以上により、与えられた座標 (x, y) の d スカラー倍の x 座標を求める処理において、 d の各ビットあたり8回の相異なる乗算処理で実現し、与えられた x 座標に対して、乱数 k により $[kx, k]$ をスカラー倍初期値とすることによって、 $d(x, y)$ 処理時間の偏差情報から秘密鍵情報がもれない方法を示した。

暗号解読DPAに対して、 $d(x, y)$ の処理電流（電圧、電力）の偏差情報から秘密鍵情報がもれない方法を示している。

【0071】

次に第5実施例を説明する。第2実施例では、射影座標を任意の $\lambda \neq 0$ について、 $[X, Y, Z] = [\lambda^2 X, \lambda^3 Y, \lambda Z]$ とするものを説明したが、 $[X, Y, Z] = [\lambda X, \lambda Y, \lambda Z]$ とする射影座標で実施することもできる。

【0072】

アフィン座標から、射影座標への変換を $(x, y) \rightarrow [x, y, 1]$ とする場合、 $Z_4 = 1$ とできる。

【0073】

＜第5実施例スカラー倍方法＞

Rのx座標の射影座標成分 X_0 、スカラー値 m を入力とし、Rの m 倍の点のx座標の射影座標成分 X_m を出力とする。 m, X_0 を入力し（ステップ1302）、乱数 k を生成し（ステップ1303）、 kX_0 を X_1 に代入する（ステップ1304）。1を Z_1 に代入する（ステップ1305）。 $[X_1, Z_1]$ を $[X_4, Z_4]$ に代入し（ステップ1306）、 $[X_1, Z_1]$ を2倍方法に入力し、出力を $[X_2, Z_2]$ へ代入する（ステップ1307）。 m の2進数表現を $h_i h_{i-1} \dots h_0$ とする。ただし、最上位ビット h_i は1である（ステップ1308）。1を i に代入する（ステップ1309）。 $i-1$ を i に代入し（ステップ1310）、 $[X_1, Z_1], [X_2, Z_2], X_4$ を加算方法に入力し、出力を $[X_3, Z_3]$ へ代入する（ステップ1311）。 $h_i = 0$ ならば、ステップ1312へ、1ならばステップ1314へ進む（ステップ1312）。 $[X_1, Z_1]$ を2倍方法に入力し、出力を $[X_1, Z_1]$ に代入する（ステップ1313）。 $[X_3, Z_3]$ を $[X_2, Z_2]$ へ代入し、ステップ1316へいく（ステップ1314）。 $[X_2, Z_2]$ を2倍方法に入力し、出力を $[X_2, Z_2]$ に代入する（ステップ1315）。 $[X_3, Z_3]$ を $[X_1, Z_1]$ へ代入し、ステップ1316へいく（ステップ1316）。 $i > 0$ ならばステップ1300へ進む（ステップ1317）。 X_1/Z_1 を X_m に代入し（ステップ1318）、 X_m を出力する（ステップ1319）。

【0074】

＜第5実施例加算方法＞

$[X_1, Z_1]$, $[X_2, Z_2]$, X_4 を入力とし、 $[X_3, Z_3]$ または無限遠点を出力とする。 $[X_1, Z_1]$, $[X_2, Z_2]$, X_4 を入力する（ステップ1402）。 $X_1 Z_2$ を S_1 に代入し（ステップ1403）、 $X_2 Z_1$ を S_2 に代入し（ステップ1404）、 $S_1 + S_2$ を B に代入する（ステップ1405）。 $B = 0$ の場合、ステップ1407へ、成立しない場合ステップ1408へ進む（ステップ1406）。無限遠点を出力し、ステップ1413へいく（ステップ1407）。次に、 B^2 を Z_3 に代入し（ステップ1408）、 $S_1 S_2$ を S に代入し（ステップ1409）、 $(X_4 B^2)$ を M に代入し（ステップ1410）、 $M + S$ を X_3 に代入し（ステップ1411）し、 $[X_3, Z_3]$ を出力する（ステップ1412）。以上により、相異なる変数の乗算4回で加算演算を実行できる。なお、2倍演算は、前述した実施例の2倍演算を利用する。尚、本実施例は2の拡大体上、素体上の楕円曲線どちらにも適用可能である。

【0075】

次に第6実施例を説明する。図1の楕円曲線演算部を、図9における901の楕円曲線演算装置で実施する。901は点のx座標 X_0 、スカラー値 m 、2の拡大体上の楕円曲線の標準形 $y^2 + xy = x^3 + ax^2 + b$ における b を入力し（902）、 m 倍の点のx座標を X_m 出力する（903）。尚、本実施例は2の拡大体上の楕円曲線で説明するが、素体上の楕円曲線を用いた場合も同様の方法で実現可能である。

【0076】

乱数生成部904は、乱数 k を生成し、 k を出力する（905）。射影座標変換部906には乱数生成部904からの乱数 k の他、x座標 X_0 とスカラー値 m 、 b を入力し（905）、射影座標 $[kX_0, k]$ に変換する。これを $[X_1, Z_1]$ とする。スカラー倍部908は射影座標 $[X_1, Z_1]$ とスカラー値 m を入力し、 $[X_1, Z_1]$ の m 倍点を求め、そのx座標 X_m を出力する。ここで、スカラー倍部908は、先ず、 $[X_1, Z_1]$ を $[X_4, Z_4]$ へ代入する。かかる $[X_4, Z_4]$ は、例えばスカラー倍部のメモリに予め記憶させておく。ま

た $[X_1, Z_1]$ を913へ出力して、2倍点 $[X_2, Z_2]$ を得る。次に、 m を2進数展開して、上位ビットからビットが0の場合 $[X_1, Z_1]$ を913に出力して913の出力である2倍点を $[X_1, Z_1]$ に代入する。その後 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ を910へ入力して出力である加算点を $[X_2, Z_2]$ に代入する。ビットが1の場合 $[X_2, Z_2]$ を913に出力して913の出力である2倍点を $[X_2, Z_2]$ に代入する。その後 $[X_1, Z_1]$ 、 $[X_2, Z_2]$ 、 $[X_4, Z_4]$ を910へ入力して出力である加算点を $[X_1, Z_1]$ に代入することにより m 倍の点の X_m 座標を得る。

【0077】

加算演算部910では、 $[X_1, Z_1]$ $[X_2, Z_2]$ $[X_4, Z_4]$ を入力し、 $[X_3, Z_3] = [X_2, Z_2] + [X_1, Z_1]$ 、 $[X_4, Z_4] = [X_2, Z_2] - [X_1, Z_1]$ となる $[X_3, Z_3]$ を以下のように求め出力する。

【0078】

まず、 $S_1 \leftarrow X_1 Z_2^2$ 、 $S_2 \leftarrow X_2 Z_1^2$ 、 $B \leftarrow S_1 + S_2$ を計算する。ここで $B = 0$ の場合、無限遠点を出力し終了となる。 $B \neq 0$ が成立しない場合、 $Z_3 \leftarrow Z_4 B$ 、 $S \leftarrow Z_4^2 S_1 S_2$ 、 $M \leftarrow X_4 Z_3^2$ 、 $X_3 \leftarrow M + S$ を計算する。

【0079】

2倍演算部913では、 $[X_1, Z_1]$ 、 b を入力し、 $[X_2, Z_2] = [X_1, Z_1] + [X_1, Z_1]$ となる $[X_2, Z_2]$ を以下のように求め出力する。すなわち、 $X_1 = 0$ または $Z_1 = 0$ の場合、無限遠点を出力する。他の場合、 $S \leftarrow Z_1^2$ 、 $Z_2 \leftarrow X_1 S$ 、 $X_2 \leftarrow X_1^4 + b(S)^4$ を計算する。

【0080】

上記実施例では、 x 座標 X_0 を射影座標 $[k X_0, k]$ に変換した例を説明したが、射影座標 $[k^2 X_0, k]$ に変換する場合にも適用可能である。

【0081】

尚、上述した実施例にかかるプログラムは記録媒体に格納しておくことも可能である。

【0082】

【発明の効果】

本発明により前記従来により、高速に楕円曲線暗号処理を実行できる。また、楕円曲線暗号の実行方法において、 $d(x, y)$ の処理時間が d のビットパターンに依存しない処理方法を与えることによって、偏差情報から秘密鍵情報がもれずに処理できる。

【図面の簡単な説明】

【図1】

本発明の楕円曲線暗号システムにおける処理の流れを示す図である。

【図2】

本発明の第1の実施例を示す楕円曲線暗号実行方法及び装置においてスカラー倍方法を示すフローチャートである。

【図3】

本発明の第1の実施例を示す楕円曲線暗号実行方法及び装置においてスカラー倍方法を示すフローチャートである。

【図4】

本発明の第1の実施例を示す楕円曲線暗号実行方法及び装置を実行するための加算演算のフローチャートである。

【図5】

本発明の第1の実施例を示す楕円曲線暗号実行方法及び装置を実行するための2倍演算のフローチャートである。

【図6】

本発明の第2の実施例を示す楕円曲線暗号実行方法及び装置においてスカラー倍方法を示すフローチャートである。

【図7】

本発明の第2の実施例を示す楕円曲線暗号実行方法及び装置においてスカラー倍方法を示すフローチャートである。

【図8】

本発明の第2の実施例を示す楕円曲線暗号実行方法及び装置を実行するための

加算演算のフローチャートである。

【図 9】

本発明の楕円曲線演算装置を構成図である。

【図 10】

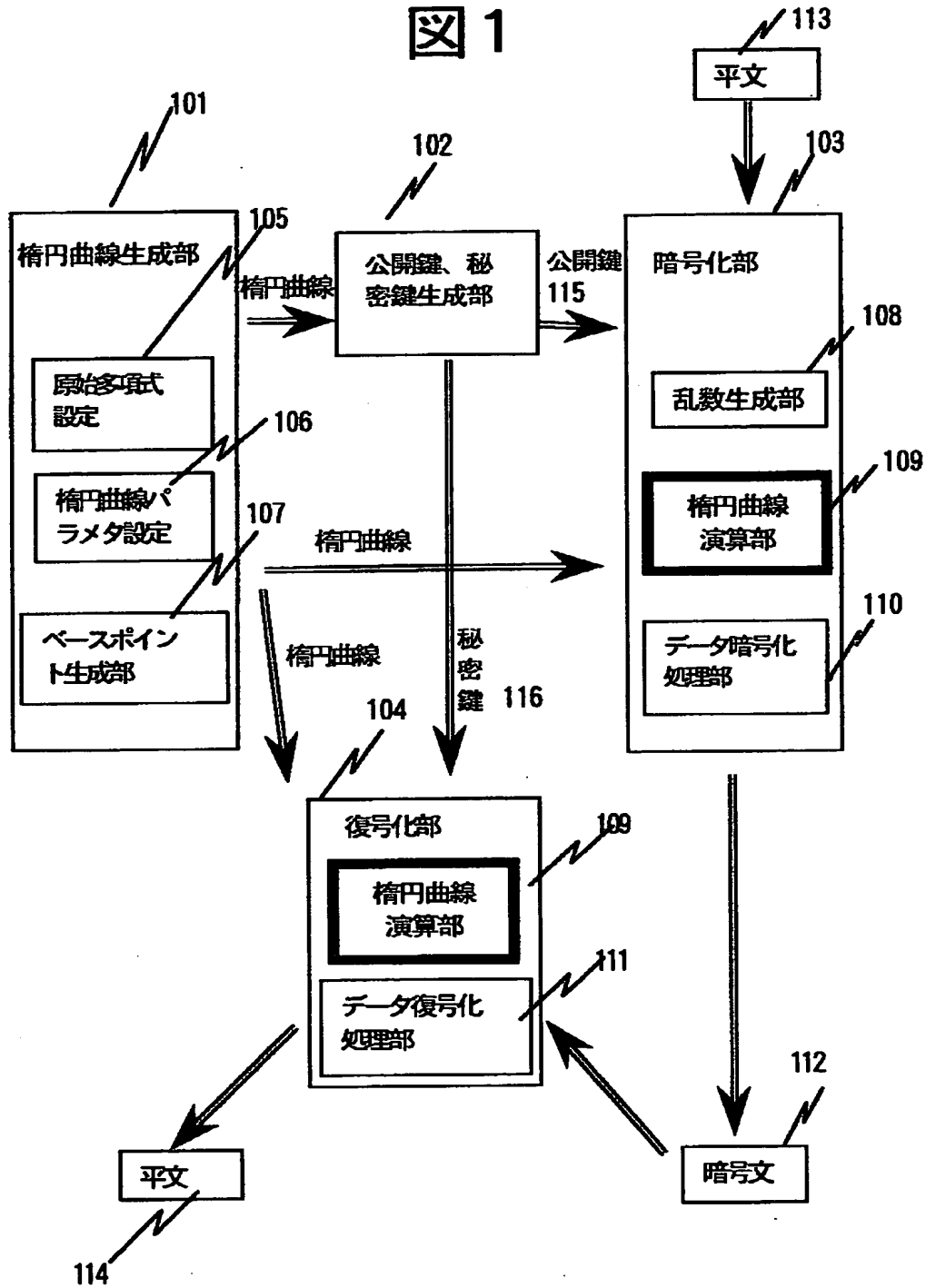
本発明の楕円曲線暗号システムの構成図である。

【符号の説明】

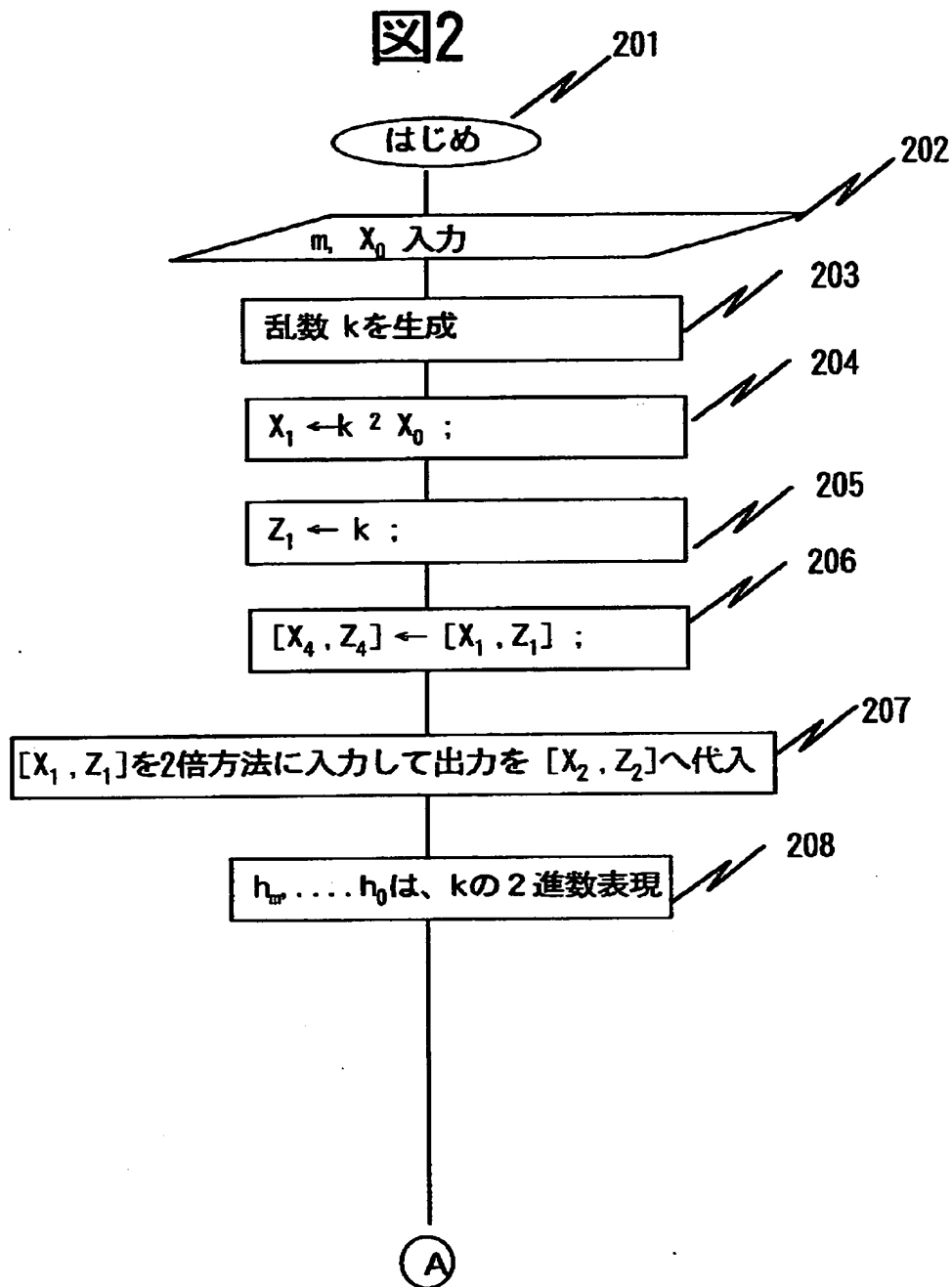
- 101 楕円曲線生成部、
- 102 公開鍵、秘密鍵生成部、
- 103 暗号化部、
- 104 復号化部、
- 105 素数生成部、
- 106 楕円曲線パラメタ設定、
- 107 ベースポイント生成部、
- 108 乱数生成部、
- 109 楕円曲線演算部、
- 110 データ暗号化処理部、
- 111 データ復号化処理部、
- 112 暗号文、
- 113 平文。

【書類名】 図面

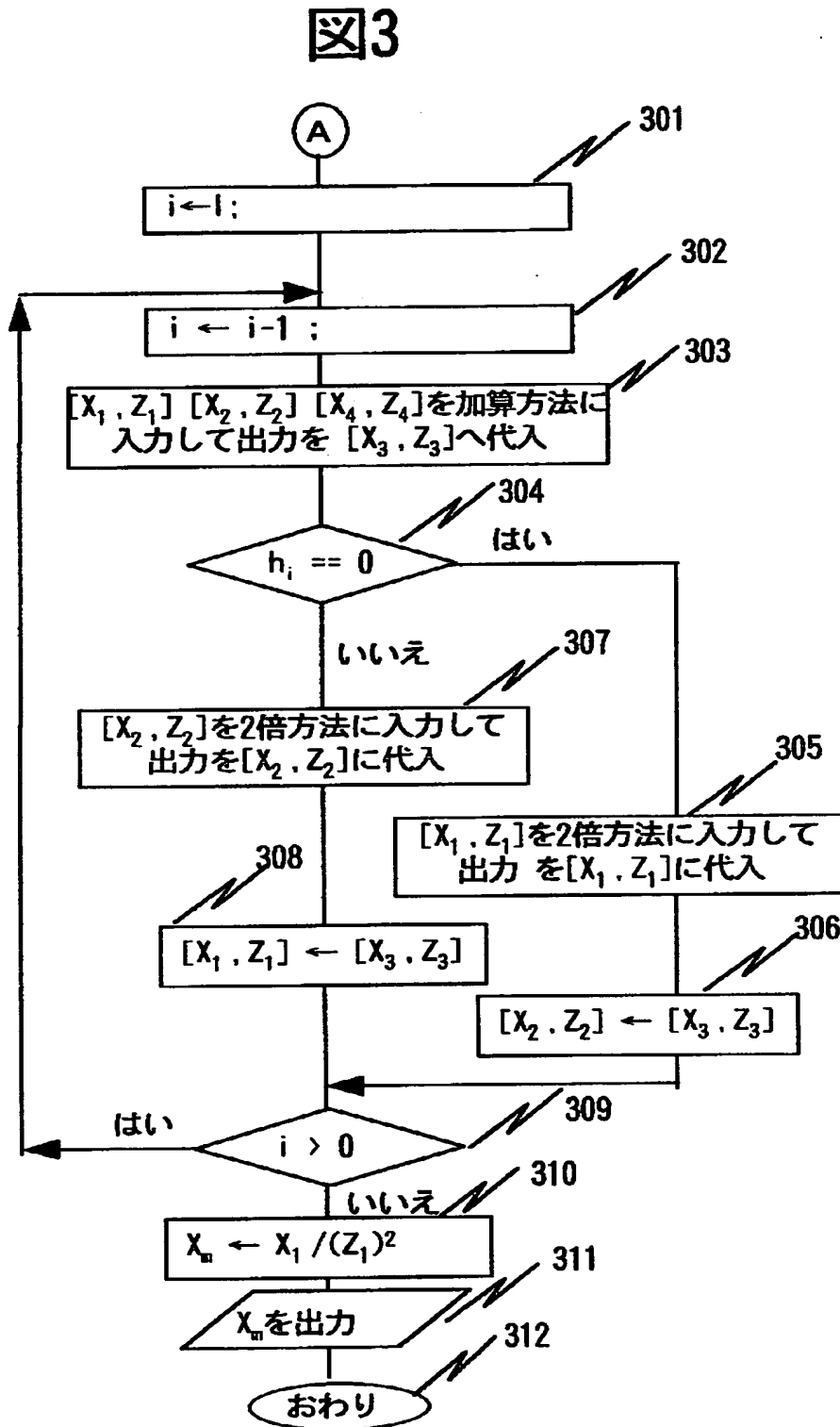
【図 1】



【図2】

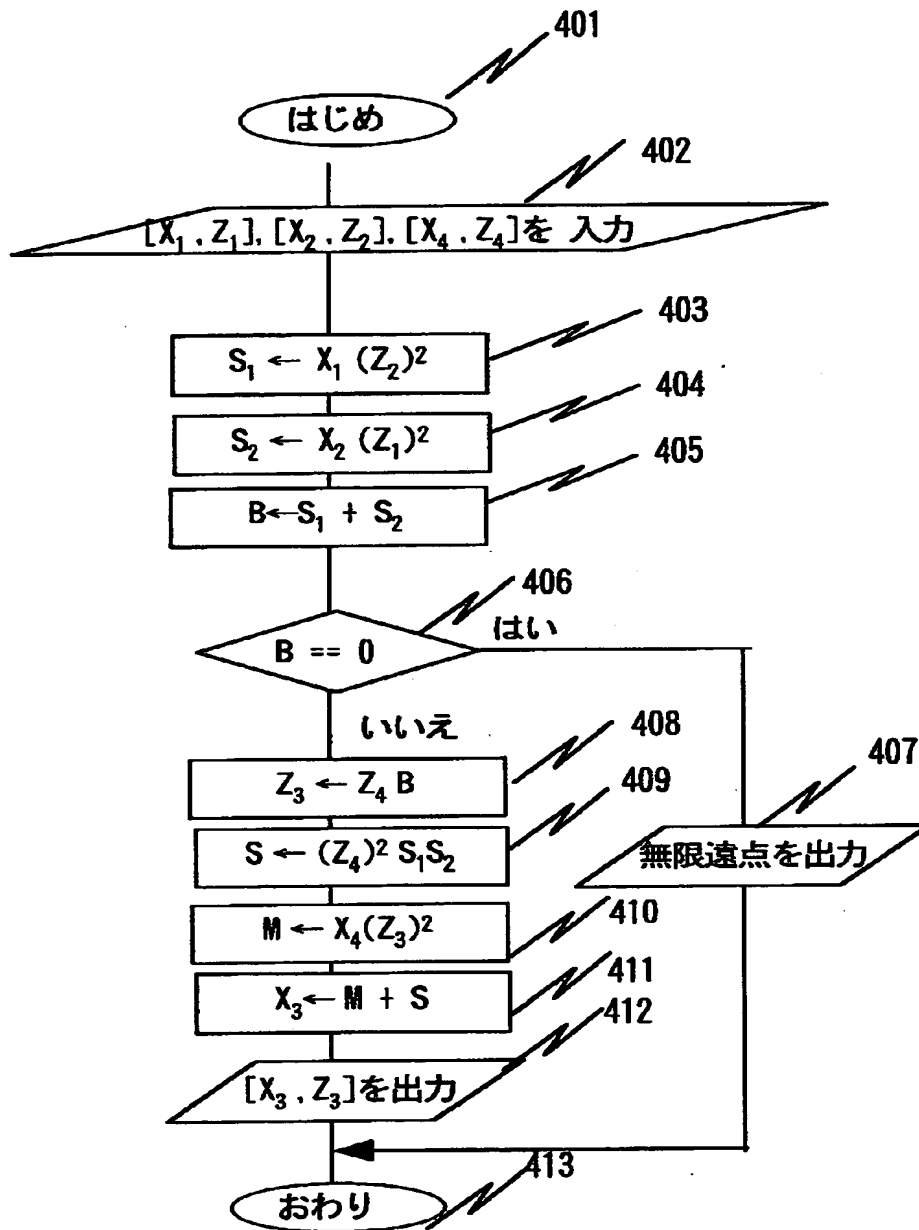


【図 3】



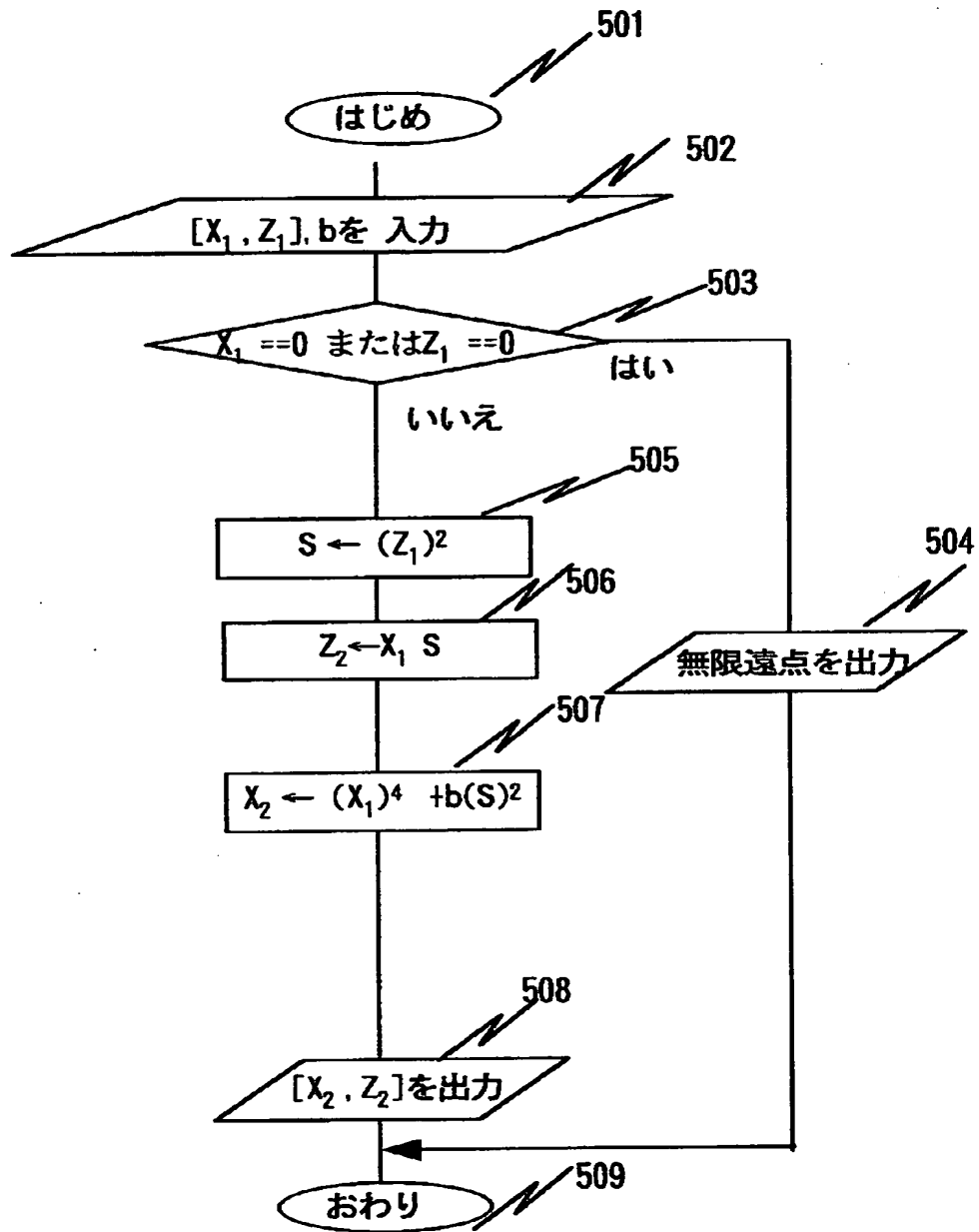
【図4】

図4

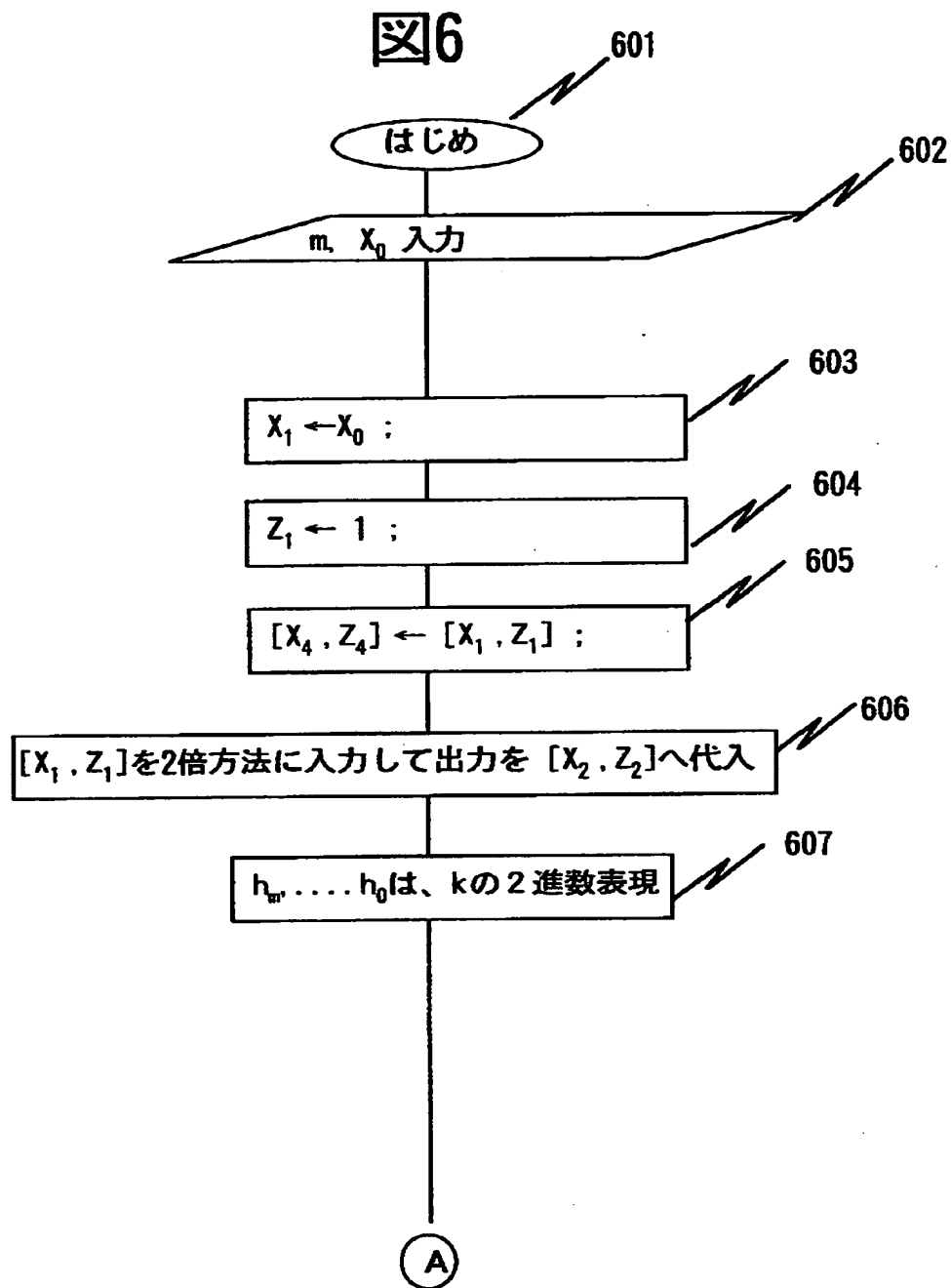


【図5】

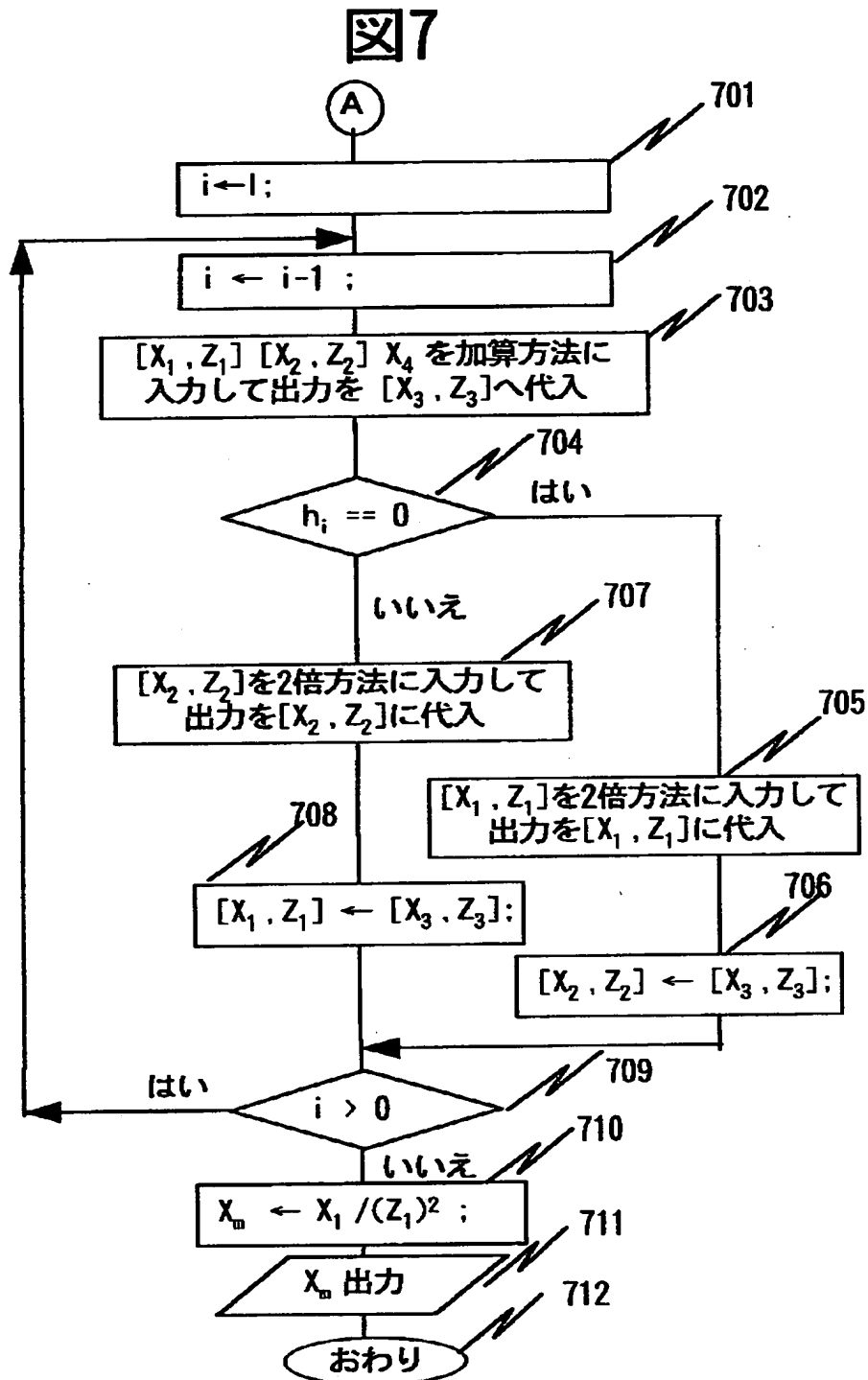
図5



【図6】

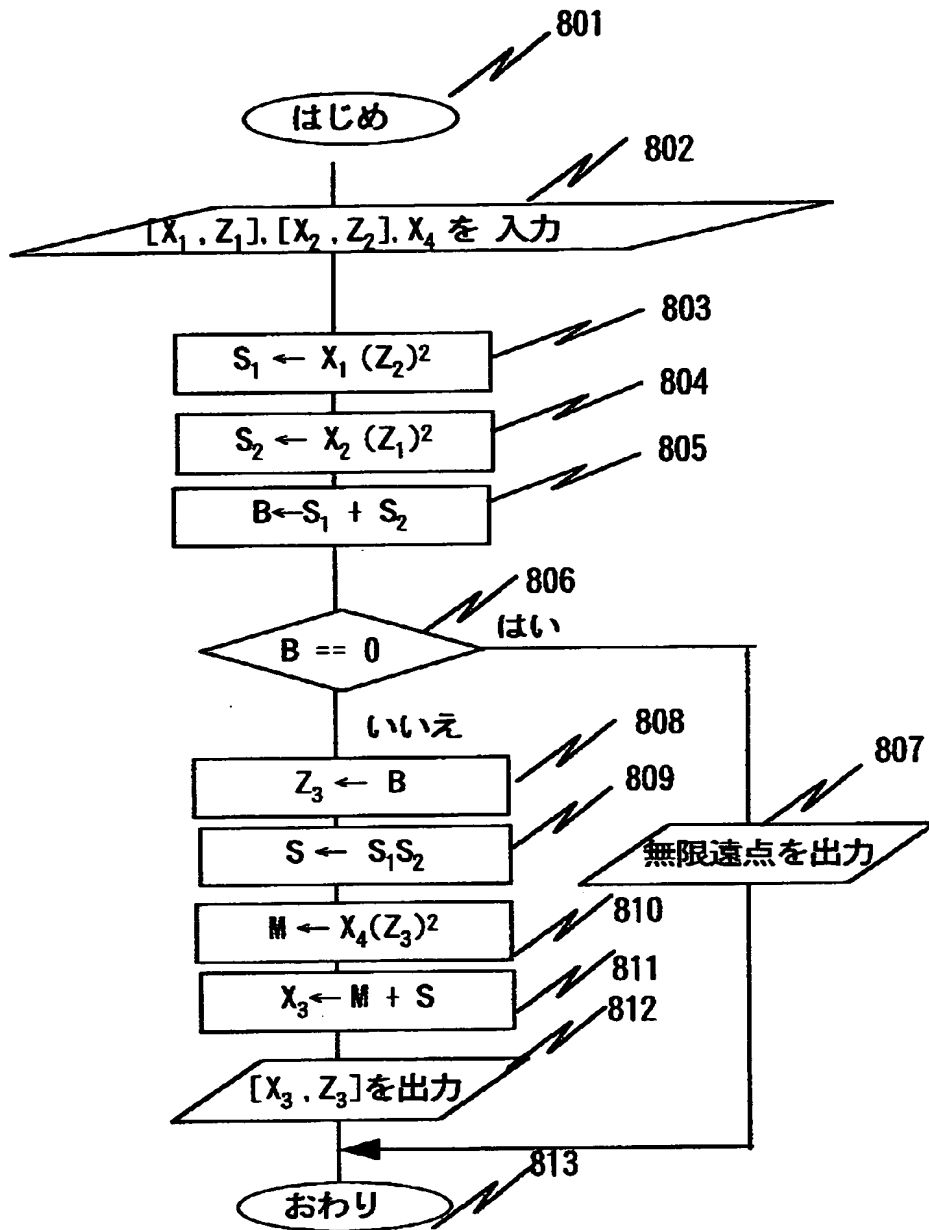


【図 7】



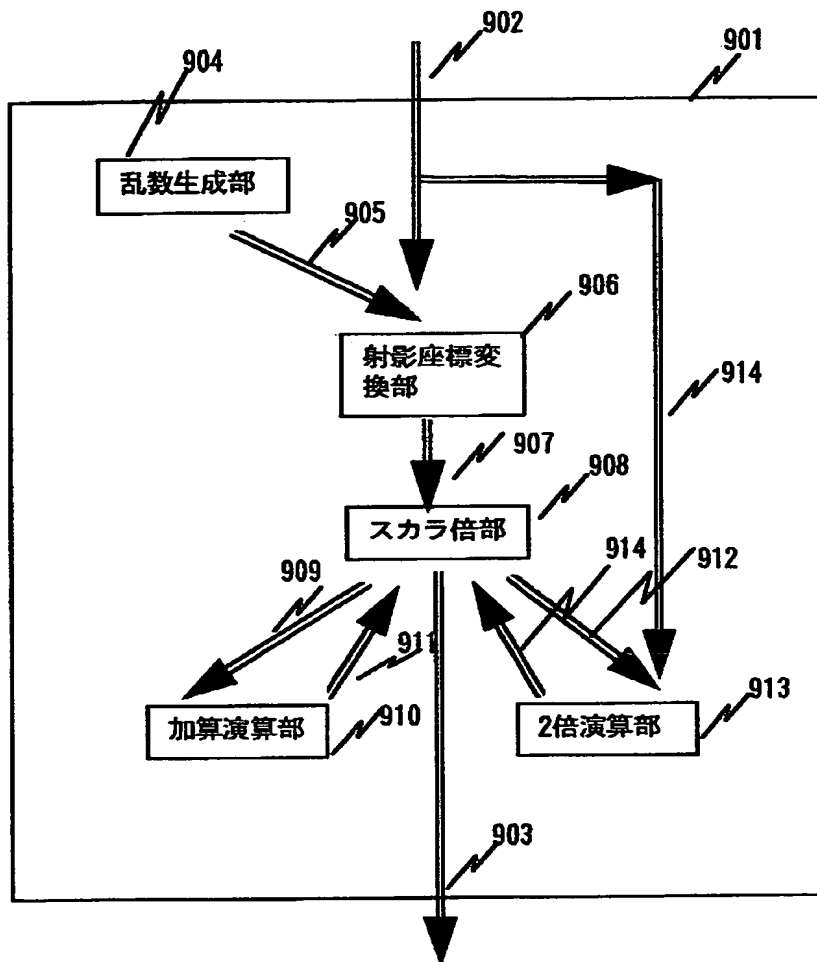
【図 8】

図8



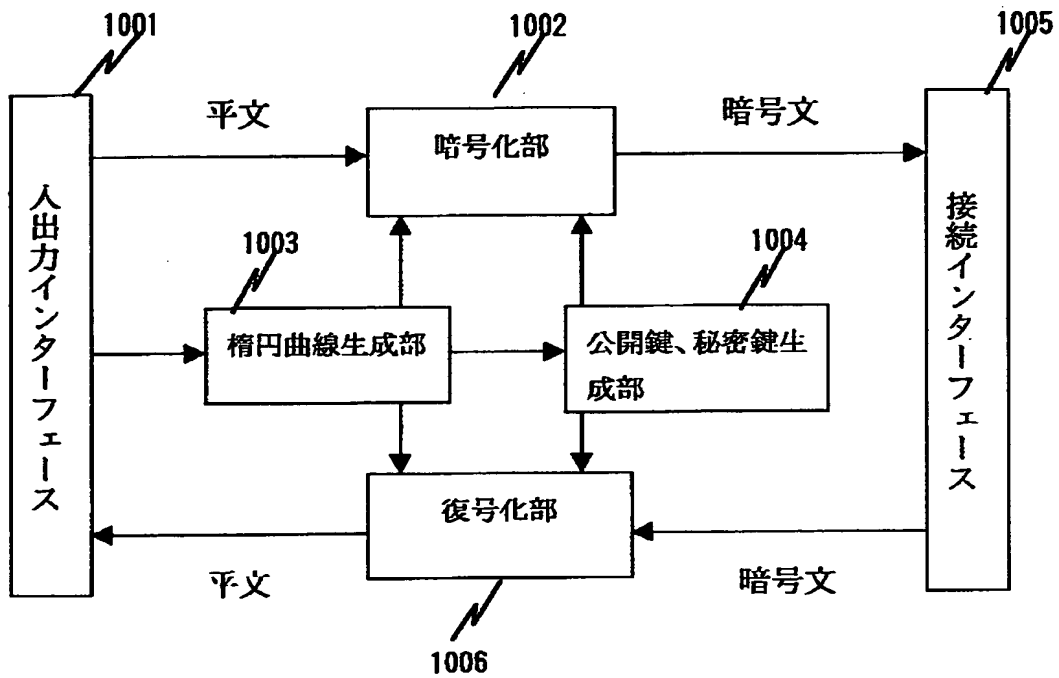
【図9】

図9



【図 10】

図 10



【書類名】 要約書

【要約】

【課題】

楕円曲線暗号処理を実行する方法は知られていたが、楕円曲線暗号のデータ復号化処理では、与えられた楕円曲線上の点 (x, y) の秘密鍵 d から、 (x, y) のスカラー倍演算 $d(x, y)$ を行う。 d の偏差情報をもれないスカラー倍演算方法で高速な方法を与える。

【解決手段】

次の手段を用いる。

(1) d のビットあたり一定の乗算回数でスカラー倍演算 $d(x, y)$ を求める方法を与える。

(2) スカラー倍 $d(x, y)$ を計算する場合、このアフィン座標 (x, y) を射影座標する際に、乱数 k を生成し、 $(x, y) \rightarrow [kx, ky, k]$ または $(x, y) \rightarrow [k^2x, k^3y, k]$ に変換する。このことにより、素体の演算対象が乱数によって変更する方法を与える。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所